

SEALED

UNITED STATES DISTRICT COURT

MAY 23 2019

for the
Western District of WashingtonJULIA C. DUDLEY, CLERK
BY: *A. Rust*
DEPUTY CLERKIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)246 Silas Gibson Drive
Big Stone Gap, VIRGINIA 24219

Case No.

2:19mj9

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See attachment A incorporated here by reference.located in the Western District of Virginia, there is now concealed (identify the person or describe the property to be seized):
See attachment B incorporated here by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251(a);	Sexual Exploitation of a Child
18 U.S.C. § 2252(a)(2);	Distribution, Receipt and Possession of Child Pornography

The application is based on these facts:
See attached affidavit in support of search warrant.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Lydia D. Adkins
Applicant's signature

Lydia D. Adkins, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/23/2019City and state: Abingdon, Virginia

Pamela Meade Sargent
Judge's signature
Pamela Meade Sargent USMT
Printed name and title

**IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF VIRGINIA
BIG STONE GAP DIVISION**

**IN THE MATTER OF THE
APPLICATION FOR A SEARCH
WARRANT FOR:**

**246 Silas Gibson Drive
Big Stone Gap, VA 24219**

)
)
)
)
)
)

Misc. No.: _____

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Lydia Denise Adkins, Special Agent with the Federal Bureau of Investigation (FBI),
Richmond Field Office, Bristol Virginia Resident Agency being duly sworn, depose and state the
following:

1. I am “an investigative or law enforcement officer” of the United States within the
meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States
who is empowered by law to conduct investigations of, and to make arrests for, offenses
enumerated in Section 2516 of Title 18, United States Code. I make this affidavit in support of
an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant
authorizing the search of the property located at 246 Silas Gibson Drive, Big Stone Gap Virginia
24219 (further described in Attachment A) and seize evidence described in Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since
2000 and currently assigned to Bristol Virginia Resident Agency, which is responsible for
conducting investigations related to a variety of violations. As a Special Agent with the FBI, I
am authorized to investigate violations of the laws of the United States, and I have participated in
numerous criminal investigations involving violations of federal law. I am a law enforcement
officer with authority to execute arrest and search warrants under the authority of the United
States. I have worked on federal corruption investigations, healthcare fraud investigations and

criminal enterprise investigations since the beginning of my employment with the FBI that have led to the arrests and convictions of numerous offenders. Prior to being employed with the FBI, from February 1994 to August 2000, I was employed as a police officer with the Johnson City Police Department, Johnson City, Tennessee. I have received training and experience in various law enforcement techniques, including interviewing and interrogation, arrest procedures, search and seizure, search warrant applications, narcotics trafficking, white collar crimes, violent crimes, kidnapping, money laundering, and various other crimes. In the course of conducting these investigations, your affiant has been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses; conducting physical surveillance; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen register and caller identification system data; conducting court-authorized electronic surveillance; and preparing and executing search warrants that have led to substantial seizures of narcotics, firearms, and other contraband.

3. The statements in this affidavit are based on information obtained from other law enforcement officers and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, the Affiant has not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that fruits, evidence and instrumentalities of crime are located in the following places or devices:

A. 246 Silas Gibson Drive, Big Stone Gap Virginia 24219 (“**Subject Premises**”)(Attachment A),

4. I make this affidavit in support of an application for a search warrant for the residence listed above, and the seizure and search of the items described in Attachment B.

5. The statements in this affidavit are based on information obtained from my observations and communications, as well as information learned from other law enforcement officers and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, the Affiant has not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that Lamont Hamilton (HAMILTON) has violated the following statutes:

- a. **Count 1: Sexual Exploitation of a Child, 18 U.S.C. § 2251(a);**
- b. **Count 2: Distribution, Receipt and Possession of Child Pornography, 18.U.S.C. § 2252(a)(2).**
- c. **Sexual Exploitation of a Child (18 U.S.C. § 2251(a)):** This statute provides that “Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or

transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed. It is also a crime to attempt to sexually exploit a child. 18 U.S.C. § 2251(e).

d. **Distributing Visual Depictions of Minors Engaged in Sexually Explicit**

Conduct: This investigation concerns also alleged violations of 18 U.S.C. § 2252(a)(2), which generally prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

6. Definitions: The following definitions apply to this Affidavit:

a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of

conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

f. The term “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

INTRODUCTION

7. [REDACTED], the mother of a minor victim in a case investigated by the [REDACTED] County Virginia Sheriff’s Office, received a telephone call from Lamont HAMILTON concerning some information HAMILTON had about the minor victim. HAMILTON is a

criminal defense attorney and represents a defendant on charges involving the minor victim. The next day, HAMILTON came the residence of [REDACTED] and gave her an envelope that contained a letter, handwritten by HAMILTON, and a number of sexually explicit printed photos of her daughter, the minor victim. HAMILTON told [REDACTED] the photos were what he had called her about and encouraged her to have a meeting with him concerning the photos.

FACTS AND CIRCUMSTANCES

8. On December 4, 2018, [REDACTED] the mother of the minor victim, received a telephone call from HAMILTON concerning some information HAMILTON had about the minor victim. HAMILTON is the criminal defense attorney for a defendant in a state case in [REDACTED] County, Virginia, involving the minor victim. [REDACTED] told HAMILTON that she did not want to speak with him or meet with him. On December 5, 2018, HAMILTON came to the residence of [REDACTED] and personally handed her an envelope labeled "Confidential [REDACTED]" that contained a hand-written letter that had been signed by HAMILTON and seventeen sexually explicit printed photographs of [REDACTED] minor daughter. HAMILTON told [REDACTED] the photos were what he had called her about and that she need to "do the right thing".

9. The letter was handwritten by HAMILTON to the attention of [REDACTED]

[REDACTED] and was signed by HAMILTON and reads as follows:

Dear [REDACTED]

It is very important that I speak with you. I'd like to set-up a time to meet so that we can get to the truth of all of this.

Enclosed is some of the additional evidence that was recently discovered. I too am a parent and I would not want my daughter to have to go through something like this. But, we need to get

to the bottom of this and the truth will come out. How it comes out, privately or publicly, will in part depend on you all.

The Commonwealth's Attorney's office can't protect your daughter if she has been untruthful, especially if it was on the witness stand and under oath. Perjury is a Felony offense. However, I believe that we can get to the truth by working cooperatively.

If you have any doubts, questions, or concerns, I'd advise you to speak with an attorney of your own. Please be advised that I can speak with you, but I can't give you any legal advice. If you would like to meet to discuss matters, please contact me as soon as you are able. You can reach me at # 276-219-8190.

Thank you,

(Signature)

Lamont Hamilton, Esq.

10. A review of the photos by law enforcement found that twelve of the printed photos depicted the minor victim in the full or partial nude, exposing the vaginal area and breasts. Four of the printed photos depicted the full or partial facial area of the minor victim. Additionally, there were two full pages and one small page of small screen shots of the minor victim. There were a total of fifteen small screen shots of the minor victim in the full or partial nude and a total of two photos of the minor victim's face found on these pages. The printed photographs measured approximately four inches by six inches and appear to be screen shots from a cell phone that have been printed on stock white paper from a home computer. The four inch by six inch photographs appear to have been printed on full size paper and were later hand trimmed.

11. On December 5, 2018, [REDACTED] met with [REDACTED] County Commonwealth's

Attorney's Office and turned over the photographs given to her by HAMILTON. Later that same day, a Virginia State Police special agent took possession of the photographs and on December 6, 2018, released the photos to agents of the Federal Bureau of Investigation.

12. On December 6, 2018, [REDACTED] placed a consensually recorded telephone call to HAMILTON at the direction of law enforcement. During the conversation, [REDACTED] asked HAMILTON where he got the photos of her daughter and HAMILTON responded, "I can't disclose where I got them". HAMILTON, again told [REDACTED] to "do the right thing".

13. Based on limited information provided by HAMILTON, [REDACTED] believed the photographs of her daughter are related to testimony her daughter provided against HAMILTON'S client, [REDACTED] during a recent state criminal trial. During a review of the handwritten letter given to [REDACTED] by HAMILTON, it is noted that HAMILTON writes "the truth will come out, how it comes out, privately or publicly, will in part depend on you all". [REDACTED] believed this is a threat from HAMILTON and is meant to intimidate the [REDACTED] family and influence the minor victim's previous and future testimony. HAMILTON further wrote in the letter delivered to [REDACTED] "The Commonwealth's Attorney's Office can't protect your daughter if she has been untruthful."

14. On December 14, 2018, [REDACTED] the parents of the minor victim, conducted a consensually recorded meeting with HAMILTON at the direction of law enforcement. The meeting took place at [REDACTED]. [REDACTED] asked HAMILTON several times throughout the meeting where he got the photos. HAMILTON would only reply by saying "do the right thing."

15. On February 22, 2019, [REDACTED] the mother of HAMILTON'S client, [REDACTED] and who the minor victim testified against, told Agents of the F.B.I. that she

was directed by her son to help HAMILTON find the photos of the minor victim that [REDACTED] had on his phone. Specifically, [REDACTED] told [REDACTED] to retrieve the phone from his previous residence, which she did, and gave [REDACTED] his usernames and password to access the phone. [REDACTED] stated that she was able to get into the phone and see the photographs of the minor victim, which she attempted to print out, but was unable to do successfully. At some point, [REDACTED] gave the cellular telephone containing the photographs of the minor victim to HAMILTON.

16. On April 10, 2019, Agents of the Federal Bureau of Investigation interviewed HAMILTON concerning his possession and distribution of the photographs of the minor victim. HAMILTON refused to answer any questions at that time related to how he obtained the photographs or how they were digitally transferred or printed. HAMILTON did agree to later meet with agents after he spoke with the Virginia State Bar ethics hotline. HAMILTON did admit that he did in fact meet with [REDACTED] and give her the handwritten letter and the photographs of the minor victim. HAMILTON stated that he operates his legal practice from the subject premise located at 246 Silas Gibson Drive, Big Stone Gap Virginia 24219. HAMILTON refused to allow agents access to his cellular telephones or provide [REDACTED]'s cellular telephone for examination.

Computers and Child Exploitation

17. **Computers and child pornography:** Computers, computer technology, cellular phones, and digital devices have revolutionized the way in which individuals interested in child pornography interact with each other. The same is true for persons having a sexual interest in minors. For example, Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant

amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls. The high technology and modern communication methods have changed this.

18. Computers, computer technology, cellular phones, and digital devices now serve multiple functions in connection with child pornography: production, communication, social networking, researching of criminal trade craft, distribution, geolocation, and storage. With the prevalence of digital cameras and electronic device with embedded cameras, the images and videos can be transferred directly between devices, locations, and persons through the use of telephone, cable, or wireless connections. Electronic contact can be made to literally millions of devices and users around the world.

19. The modern ability to store images and videos in digital form provides an ideal repository for child pornography. The size of the electronic storage media used in home computers, digital devices, and camera is has grown tremendously within the last several years. These items can store thousands of images at very high resolution.

20. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

21. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, and live.com, among others. Online services allow a user to set up an account

with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer, phone, or digital device with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computers, phones, and devices. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's equipment or online accounts in most cases.

As is the case with most digital technology, relevant communications can be saved or stored for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Retained messages in cellular phones are another example. In addition to electronic communications, a user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer, phone or device contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

Digital Evidence

22. Digital Evidence: Searches and seizures of evidence from computers, cellular phones, and digital devices commonly require agents to download or copy information, or seize

most or all items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

23. Digital storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all of the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

24. Searching computer systems and digital devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of hardware and software available requires even experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system or digital device is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

25. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of image or movie files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues.

In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

26. In addition, there is probable cause to believe that the personal property and items described in Attachments B1 and B2, are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

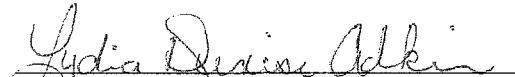
27. **Computer Data:** Based on conversations with other law enforcement officers and others with experience in executing and reviewing search warrants relating to computer crimes, I have learned that search warrants for computer systems and related data have revealed stored data many years prior to the date of the search. This observation is supported by the results of hundreds of computers, phones and digital devices in child exploitation and child pornography cases over many years in support of multiple federal, state and local investigations. In many cases, examiners have observed that forensic evidence of child pornography collecting, relevant communications, and file handling may be recovered many years after the date of the actual communication.

28. In *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012), the Seventh Circuit Court of Appeals held that concerns with staleness in child pornography cases reflect a misunderstanding of computer technology.” *Id.* at 776. *Seiver* criticized other decisions for “laboring under the misapprehension that deleting a computer file destroys it, so that if the defendant had deleted the pornographic images between their uploading to the Internet and the search of his computer the search would not have yielded up the images, or evidence of their earlier presence in the computer.” *Id.* Specifically, the Seventh Circuit explained that when a

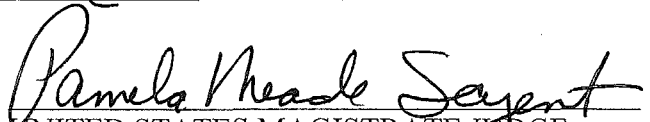
person deletes a file, it goes into a “trash” folder, and when they direct the computer to “empty” the trash folder the contents of the folder, including the deleted file, disappear. But the file may not have left the computer. The trash folder is like a wastepaper basket with no drainage pipe to the outside. The file seems to have vanished only because the computer has removed it from the user interface and so the user can’t “see” it any more. But it may still be there, and normally is recoverable by computer experts until it’s overwritten because there is no longer unused space in the computer’s hard drive. Therefore, while “Staleness” may be highly relevant to the legality of a search for a perishable or consumable object, like cocaine, it is rarely relevant when it is a computer file. Computers and computer equipment are not the type of evidence that rapidly dissipates or degrades. Because of overwriting, it is possible that the deleted file will no longer be recoverable from the computer’s hard drive. And it is also possible that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater these possibilities. But rarely will they be so probable as to destroy probable cause to believe that a search of the computer will turn up the evidence sought; for probable cause is far short of certainty—it requires only a probability or substantial chance of criminal activity, not an actual showing of such activity. In *Siever*, seven months was too short a period to reduce the probability that a computer search will be fruitful to a level at which probable cause has evaporated. Finally, the Seventh Circuit stated that the most important thing to keep in mind for future cases is the need to ground inquiries into “staleness” and “collectors” in a realistic understanding of modern computer technology and the usual behavior of its users. Only in the exceptional case should a warrant to search a computer for child pornography be denied on either of those grounds. *Id.* at 776-78 (original emphases) (citations omitted).

29. **Conclusion:** Based upon the contents of this Affidavit, I respectfully request that the Court issue a search warrant for the Subject Premises, which is more particularly described in **Attachments A1** and the seizure and search of the items described in **Attachment B**. I also submit there is probable cause to believe that HAMILTON transmitted, transported and distributed photos of a minor engaged in sexually explicit conduct by utilizing cellular telephone, computers and printers located at the Subject Premise. This conclusions is based upon his actions and statements described above. Accordingly, a search warrant is requested.

REQUEST TO SEAL: Because the Investigation is ongoing, I would request the Court to seal the Application for Search Warrant, the Search Warrant, and supporting Affidavit in this matter.


Lydia Denise Adkins, Special Agent
Federal Bureau of Investigation
United States Department of Justice

Sworn to and subscribed before me this 23rd day of May, 2019


UNITED STATES MAGISTRATE JUDGE
FOR THE WESTERN DISTRICT OF VIRGINIA

Reviewed by
M. Suzanne Kerney-Quillen
Special Assistant United States Attorney

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

246 Silas Gibson Road, Big Stone Gap, Virginia 24219 is described as a one-story single family residence on the west side of Veteran Memorial Highway. The house has red brick siding with white trim and a white front door. There is a black wooden fence around the front of the property. The numbers '246' are affixed to the center of the front door.

ATTACHMENT B

Items and Information to be Seized and Searched

1. Cellular phones, computers and computer equipment, digital storage devices, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, flash drives, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, computer software, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, or other visual depictions of such Graphic Interchange format equipment, and the data stored within these materials, which has been used or may be used for the following:

A. to visually depict minors engaged in sexually explicit conduct, child pornography, and/or child erotica;

B. to advertise, transport, distribute, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct, child pornography, and/or child erotica;

C. to show or evidence a sexual interest in minors or desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct or child pornography; and to extort or threaten the adult and minors by injuring their reputation of the reputation of another person.

2. Any and all photographs, compact disks, DVDs, motion picture films (including but not limited to 8mm film), super 8 video, video cassette tapes, production and reproduction equipment, motion picture cameras, video cameras, video cassette recorders, and other

photographic and video recording equipment used to produce or reproduce photographs, motion picture films, or video cassettes, cameras, documents, books, records, ledgers, correspondence, receipts, magazines and other materials reflecting the purchase, sale, trade, transmission, advertising, transport, distribution, receipt and possession of any visual depiction of minors engaged in sexually explicit conduct or to show or evidence a sexual interest in minors or desire or motive to collect, distribute, and receive visual depictions of minors engaged in sexually explicit conduct or child pornography.

3. Any and all magazines, books, photographs, letters, written narratives and computer text files or any other printed or electronic matter that show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct or child pornography.

4. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the residential/business premises described as and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, child pornography, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on magnetic media such as tape, cassette, disk, diskette, or on memory storage devices, such as optical disks, or storage media.

5. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct or child pornography, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect

and possess visual depictions of minors engaged in sexually explicit conduct or child pornography.

6. Records or other items that evidence ownership or use of computer equipment found in the above residence, including, but not limited to, correspondence, sales receipts, and bills for Internet access, all handwritten notes, and handwritten notes in computer manuals.

7. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of visual depictions of minors engaging in sexually explicit conduct or child pornography.

8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular phones, camera, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

A. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs and correspondence;

B. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

C. evidence of the lack of such malicious software;

D. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

E. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

F. evidence of the times the COMPUTER was used;

G. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

H. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

I. records of or information about Internet Protocol addresses used by the COMPUTER;

J. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

K. contextual information necessary to understand the evidence described in this attachment.

9. Routers, modems, and network equipment used to connect computers to the Internet;

10. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence;

11. Documents and records regarding the ownership and/or possession of the searched premises;
12. Credit card information, bills, and payment records;
13. Information or correspondence pertaining to affiliation with any child exploitation websites;
14. Definitions:
 - A. As used herein, the terms “records” and “information” refer to all forms of creation or storage, any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, videotapes, motion pictures, or photocopies).
 - B. The term “computer” refers to all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions: desktop computers, notebook computers, mobile phones, tablets, server computers, smart phones, and network hardware.
 - C. The term “storage medium” refers to any physical object upon which computer data can be recorded. Examples are hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
15. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items there.
16. Search and seizure of information/data believed to be evidence (described below) of the crime(s) of child exploitation and/or possession of child pornography involving by the user on his person, in his residence, or concealed in the described vehicle.

17. Further, a forensic analysis shall be authorized for the item seized for the purposes of recovering text messages, digital images, pictures and/or any other data of the above described incident and any and all passwords needed to access any digital media found on this search. To seize and to remove the items described above in order to allow the contents of the items to be further searched at an off-site location; To use Mobile Device Acquisition, which is the process of imaging or otherwise obtaining information from a mobile device and its associated media; to extract data from such devices, as well as from devices on which the examiner is unable to bypass a user's lock using the below described methods, when the device is damaged beyond repair, or for devices from which an examiner is unable to obtain a physical acquisition through the previously described means, more advanced methods of extraction may be necessary, including chip-off forensics. Chip-off forensics is a technique used after all other acquisition methods have been exhausted. Chip-Off forensics is a technique in which the device is disassembled and the Ball Grid Array (BGA) or memory chip is removed from the device's printed circuit board, the memory chip is cleaned and repaired and raw data is extracted from the chip using specialized tools. This process renders the mobile device unusable, but preserves the data content. In some instances, a mobile device may be damaged to an extent that extraction of data from the device or other analysis of the device in its current state would not be possible. This Affiant is requesting authorization for the examiner, or a qualified third-party, to make any necessary repairs to such devices as necessary to allow for examination of the device.

18. Any and all passwords needed to access any digital media found on this search.

SEALED

UNITED STATES DISTRICT COURT

for the
Western District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)246 Silas Gibson Drive,
Big Stone Gap, VIRGINIA 24219

Case No.

2:19mj9

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of Virginia
(identify the person or describe the property to be searched and give its location):

See attachment A incorporated here by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See attachment B incorporated here by reference.

YOU ARE COMMANDED to execute this warrant on or before June 6, 2019 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Pamela Meade Sargent
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☒ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .Date and time issued: 5/23/19 @ 2:29 p.m.City and state: Abingdon, VAPamela Meade Sargent
Judge's signaturePamela Meade Sargent, USMJ
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

246 Silas Gibson Road, Big Stone Gap, Virginia 24219 is described as a one-story single family residence on the west side of Veteran Memorial Highway. The house has red brick siding with white trim and a white front door. There is a black wooden fence around the front of the property. The numbers '246' are affixed to the center of the front door.

ATTACHMENT B

Items and Information to be Seized and Searched

1. Cellular phones, computers and computer equipment, digital storage devices, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, flash drives, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, computer software, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, or other visual depictions of such Graphic Interchange format equipment, and the data stored within these materials, which has been used or may be used for the following:

A. to visually depict minors engaged in sexually explicit conduct, child pornography, and/or child erotica;

B. to advertise, transport, distribute, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct, child pornography, and/or child erotica;

C. to show or evidence a sexual interest in minors or desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct or child pornography; and to extort or threaten the adult and minors by injuring their reputation of the reputation of another person.

2. Any and all photographs, compact disks, DVDs, motion picture films (including but not limited to 8mm film), super 8 video, video cassette tapes, production and reproduction equipment, motion picture cameras, video cameras, video cassette recorders, and other

photographic and video recording equipment used to produce or reproduce photographs, motion picture films, or video cassettes, cameras, documents, books, records, ledgers, correspondence, receipts, magazines and other materials reflecting the purchase, sale, trade, transmission, advertising, transport, distribution, receipt and possession of any visual depiction of minors engaged in sexually explicit conduct or to show or evidence a sexual interest in minors or desire or motive to collect, distribute, and receive visual depictions of minors engaged in sexually explicit conduct or child pornography.

3. Any and all magazines, books, photographs, letters, written narratives and computer text files or any other printed or electronic matter that show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct or child pornography.

4. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the residential/business premises described as and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, child pornography, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on magnetic media such as tape, cassette, disk, diskette, or on memory storage devices, such as optical disks, or storage media.

5. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct or child pornography, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect

and possess visual depictions of minors engaged in sexually explicit conduct or child pornography.

6. Records or other items that evidence ownership or use of computer equipment found in the above residence, including, but not limited to, correspondence, sales receipts, and bills for Internet access, all handwritten notes, and handwritten notes in computer manuals.

7. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of visual depictions of minors engaging in sexually explicit conduct or child pornography.

8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular phones, camera, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

A. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs and correspondence;

B. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

C. evidence of the lack of such malicious software;

D. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

E. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

F. evidence of the times the COMPUTER was used;

G. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

H. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

I. records of or information about Internet Protocol addresses used by the COMPUTER;

J. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

K. contextual information necessary to understand the evidence described in this attachment.

9. Routers, modems, and network equipment used to connect computers to the Internet;

10. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence;

11. Documents and records regarding the ownership and/or possession of the searched premises;
12. Credit card information, bills, and payment records;
13. Information or correspondence pertaining to affiliation with any child exploitation websites;
14. Definitions:
 - A. As used herein, the terms “records” and “information” refer to all forms of creation or storage, any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, videotapes, motion pictures, or photocopies).
 - B. The term “computer” refers to all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions: desktop computers, notebook computers, mobile phones, tablets, server computers, smart phones, and network hardware.
 - C. The term “storage medium” refers to any physical object upon which computer data can be recorded. Examples are hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
15. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items there.
16. Search and seizure of information/data believed to be evidence (described below) of the crime(s) of child exploitation and/or possession of child pornography involving by the user on his person, in his residence, or concealed in the described vehicle.

17. Further, a forensic analysis shall be authorized for the item seized for the purposes of recovering text messages, digital images, pictures and/or any other data of the above described incident and any and all passwords needed to access any digital media found on this search. To seize and to remove the items described above in order to allow the contents of the items to be further searched at an off-site location; To use Mobile Device Acquisition, which is the process of imaging or otherwise obtaining information from a mobile device and its associated media; to extract data from such devices, as well as from devices on which the examiner is unable to bypass a user's lock using the below described methods, when the device is damaged beyond repair, or for devices from which an examiner is unable to obtain a physical acquisition through the previously described means, more advanced methods of extraction may be necessary, including chip-off forensics. Chip-off forensics is a technique used after all other acquisition methods have been exhausted. Chip-Off forensics is a technique in which the device is disassembled and the Ball Grid Array (BGA) or memory chip is removed from the device's printed circuit board, the memory chip is cleaned and repaired and raw data is extracted from the chip using specialized tools. This process renders the mobile device unusable, but preserves the data content. In some instances, a mobile device may be damaged to an extent that extraction of data from the device or other analysis of the device in its current state would not be possible. This Affiant is requesting authorization for the examiner, or a qualified third-party, to make any necessary repairs to such devices as necessary to allow for examination of the device.

18. Any and all passwords needed to access any digital media found on this search.